DARTMOUTH DENTAL PRACTICE
24 Victoria Road
Dartmouth
Devon
Marian Roberts BDS (Sheffield) GDC61688 TQ6 9SA
Aleksander Srokosv BDS (Plymouth) GDC258317 01803 835 418
admin@dartmouthdental.co.uk www.dartmouthdental.co.uk

Business Continuity Planning
Introduction

Information Governance Requirement Number 14.1-319

1. Business Continuity Plans (BCP) represent an attempt by organisations to predict, assess and counteract threats and risks that may lead to events that seriously disrupt or curtail all or part of their business functions. Business Continuity assessments analyse the probability of untoward events occurring, their likely impacts, determine what the organisation can do if they happen, and how the organisation systematically goes about recovering from these events.
2. Organisations are likely to require support from their commissioning organisation to put appropriate plans and procedures in place.

Purpose of Business Continuity Planning

3. Business continuity planning enables an organisation to:
   - 3.1. assess the risks of a security failure or disaster occurring;
   - 3.2. analyse the consequences to the running of the organisation if a security failure or disaster was to occur;
   - 3.3. plan measures to reduce the likelihood of a security failure or disaster occurring;
   - 3.4. plan measures to allow the organisation to continue to function if a security failure or disaster does occur.
4. A senior staff member should oversee risk assessments and coordinate an overall assessment plan for the organisation.

Critical Information Systems

5. Critical information systems should include all systems containing patient/service user data and communication systems necessary for transmitting patient/service user information. Critical processes should include those necessary for delivering patient/service user care.
6. Risks to the confidentiality, integrity and availability of systems and processes should be assessed. The impact of threats should be assessed to determine priorities and plans put in place to counter the threats. Critical times (those affecting the potential to deliver adequate patient/service user care) should be assessed and countermeasures put in place to ensure system or process recovery occurs within agreed time limits.
7. Plans should be tested as table-top exercises and walk-throughs (such as validation of data back-ups).
8. Review groups should be established to take responsibility for review, coordination and testing of the plans. A regular review and testing timetable should be established, with both being conducted on an annual basis. Reviews should also be carried out following significant system changes, relocation of facilities and staff reorganisation.

DARTMOUTH DENTAL PRACTICE
24 Victoria Road
Dartmouth
Devon
Marian Roberts BDS (Sheffield) GDC61688 TQ6 9SA
Aleksander Srokosv BDS (Plymouth) GDC258317 01803 835 418
admin@dartmouthdental.co.uk www.dartmouthdental.co.uk

9. The senior management team should assess the ability of their plans to meet their objectives. If necessary an external review may be sought.

Information Security and Business Continuity Planning Terminology

- **Risk assessment**: Assessment of threats, impacts and vulnerabilities on organisational services and assets to enable measures to be taken to reduce the identified risks.
- **Disaster**: Accidental, natural or malicious events, which threaten or disrupt normal operations or services for sufficient time to have significant effects on the organisation's business.
- **Threat**: A potential cause of an unwanted incident, which may result in harm to a system or organisation.
- **Confidentiality**: Ensuring that information is accessible only to those authorised to have access.
- **Integrity**: Safeguarding the accuracy and completeness of data and information and processing methods.
- **Availability**: Ensuring that authorised users have access to information and associated assets when required.

Business continuity plan. Wherever possible systems are replicated on a regular basis to provide back-up should there be a breach of security, data loss, equipment failure or break-in. In all of these cases we have attempted to provide a contingency plan to recover data wherever possible in the minimum amount of down-time.

Romexis - X-ray and photographic patient data. Theses system are continuously backed up from our server to a secondary system. This system is also backed-up to a second source. If there were physical loss/damage/failure then a 'cloud-based' backup is accessible.

Dentally - patient management software. Dentally is web-based and all files are backed up on secure servers. 2 factor authentication is required to log-on to the system.

Dartmouth Dental Practice - electronic files. We use '**Dropbox**' for file sharing. This is a cloud-based system.

Actionees

Keith Roberts, Laura White and Marian Roberts